D Infrastruktur, Betrieb und Werkzeugunterstützung

15 Standards/IT-Frameworks zur Sicherstellung der IT-Compliance Konformität in hochflexiblen Geschäftsprozessen

Stephan Weber, Dieter Bartmann

Zusammenfassung. In hochflexiblen Geschäftsprozessen (hGP) ist die Sicherstellung eines einheitlichen und damit vergleichbaren IT-Compliance-Niveaus eine der zentralen Herausforderungen, welcher mit der Anwendung von Standards/IT-Frameworks begegnet werden kann. Anhand eines definierten Anforderungskatalogs hat die Analyse von vier ausgewählten Standards/IT-Frameworks ergeben, dass CobiT insbesondere im Kontext von hGP einen hilfreichen Beitrag zur Gewährleistung der IT-Compliance Konformität leisten kann. Jedoch schränkt die alleinige Fokussierung auf CobiT die Flexibilität zu stark ein. Die Anwendung einer Policy kann hierfür Abhilfe schaffen.

15.1 Problemstellung, Zielsetzung und Aufbau

Um im Wettbewerb dauerhaft erfolgreich zu bestehen, ist es unabdingbar, auf unvorhersehbare Ereignisse und ad-hoc getroffene Entscheidungen, wie z. B. die Erschließung neuer Märkte, die rasche Etablierung einer Kooperation zwischen Unternehmen oder neue bzw. geänderte Gesetze und Regularien, flexibel und schnell reagieren zu können. Neben der technischen Herausforderung muss aber auch zugleich die gesetzeskonforme IT-Ausgestaltung gewährleistet werden.

Zur Sicherstellung eines einheitlichen IT-Compliance-Niveaus vor allem in Föderationen ist folgende Problemstellung zu bewältigen: Wie kann eine Vergleichbarkeit zwischen den einzelnen teilnehmerspezifischen Aussagen zur IT-Compliance hergestellt werden? In diesem Zusammenhang kommt erschwerend hinzu, dass sowohl der Gesetzgeber als auch die Aufsichtsorgane zunehmend eine Abkehr von der traditionell Regel-basierten Aufsicht hin zu einer Prinzipien-basierten Aufsicht vollziehen, d. h. den Unternehmen wird in Form von sehr generalistisch gehaltenen Empfehlungen bzw. Handlungsanweisungen bewusst mehr Gestaltungsspielraum für die Erfüllung der entsprechenden Gesetze und Regularien gegeben (Bretz et al. 2007, S. 3). Damit wird dem Grundsatz der

Verhältnismäßigkeit Rechnung getragen. So wird z. B. das Wort „angemessen“ im § 9 BDSG (Bundesdatenschutzgesetz 2009) von Unternehmen unterschiedlicher Größe und Komplexität auch unterschiedlich ausgelegt. Als Konsequenz sind somit auch die jeweiligen unternehmensspezifischen Regelungen und Richtlinien entsprechend mehr oder weniger scharf bzw. restriktiv formuliert. Diese Unschärfe ist bei organisations- bzw. unternehmensübergreifenden Geschäftsprozessen besonders problematisch, denn es gilt der Grundsatz: „Eine Kette ist nur so stark wie ihr schwächstes Glied“.

In hierarchischen, starren Verbundstrukturen, in denen jeder Teilnehmer vorab bekannt ist, kann dieser Problemstellung mit der zwingenden Vorgabe der Verwendung eines oder mehrerer Standards bzw. IT-Frameworks begegnet werden.

Jedoch erfordern die eingangs erwähnten Herausforderungen zunehmend flexible bzw. hochflexible Geschäftsprozesse (hGP). Diese lassen sich anhand der drei Merkmale (1) Kontextsensitivität, (2) unvollständige Planbarkeit und (3) Überlappung von Planung und Ausführung charakterisieren (Pütz et al. 2009, S. 1). Gerade aufgrund der Unvorhersehbarkeit als übergreifender Aspekt der aufgeführten hGP-Merkmale lässt sich die gleiche Lösung wie bei starren Strukturen nicht anwenden, da die Teilnehmer und damit auch ihre verwendeten Standards/IT-Frameworks in einer sich ad-hoc bildenden Föderation vorab nicht bekannt sind.

Die Zielsetzung des vorliegenden Beitrags besteht darin, eine Policy für die Problemstellung „Sicherstellung eines einheitlichen IT-Compliance-Niveaus im hGP-Kontext“ zu entwickeln. Mit deren Hilfe kann eine ad-hoc Entscheidung getroffen werden, ob ein kurzfristig auftretender neuer potenzieller Teilnehmer an der Föderation teilnehmen darf, ohne das bestehende IT-Compliance-Niveau zu gefährden.

Dazu werden auf Basis von definierten Anforderungen vier ausgewählte Standards bzw. IT-Frameworks auf ihre Eignung im Kontext von hGP untersucht. Weiterhin wird den Fragestellungen nachgegangen, wie die Situation zu behandeln ist, wenn mehrere verschiedene Standards/IT-Frameworks in einem sich ad-hoc bildenden Wertschöpfungsnetz verwendet werden und welche Möglichkeiten bestehen, die Korrektheit der gemachten Angaben zu gewährleisten.

Der Aufbau des Beitrags gestaltet sich wie folgt: Abschnitt 15.2 beinhaltet zunächst eine kritische Auseinandersetzung mit den Begrifflichkeiten „IT-Compliance, Norm, Standard, IT-Framework“ und zur inhaltlichen Konkretisierung von IT-Compliance eine Darstellung ausgewählter, branchenunspezifischer

IT-Compliance-Anforderungen. Zudem werden allgemeine Konsequenzen bei Verletzung bzw. Nichteinhaltung von IT-Compliance-Vorschriften sowie die Schwierigkeiten bei deren Umsetzung insbesondere im Kontext von hGP aufgezeigt. Die Definition des Anforderungskatalogs für Standards/IT-Frameworks unter Beachtung der Eigenschaften von hGP ist Inhalt von Abschnitt 15.3. Im nachfolgenden Abschnitt 15.4 werden vier ausgewählte Standards bzw. IT-Frameworks kurz dargestellt. In Abschnitt 15.5 erfolgt die Bewertung der vorgestellten Standards/IT-Frameworks anhand der spezifizierten Anforderungen. Die Anwendung der erzielten Ergebnisse auf das Szenario e-Car Net wird in Abschnitt 15.6 veranschaulicht. Abschließend liefert Abschnitt 15.7 eine Zusammenfassung über die gewonnen Erkenntnisse.

15.2 Grundlagen

In diesem Abschnitt erfolgt zunächst eine Definition von grundlegenden Begrifflichkeiten, um ein einheitliches Verständnis zu schaffen. Im Anschluss daran werden einige ausgewählte IT-Compliance-Anforderungen dargestellt und mögliche Auswirkungen aufgrund der Nichteinhaltung von IT-Compliance-Vorschriften sowie Herausforderungen bei deren Umsetzung thematisiert.

15.2.1 Begriffsbestimmungen

Dieser Abschnitt beinhaltet eine detaillierte Erklärung und Abgrenzung der Begriffe „IT-Compliance“, „Norm“, „Standard“ und „IT-Framework“.

IT-Compliance

In der Literatur sind verschiedene Definitionen zu finden, die den Begriff unterschiedlich stark eingrenzen. Im Folgenden werden einige davon aufgezeigt, um diesen Sachverhalt darzustellen.

Der Begriff „Compliance“ stammt aus dem Englischen und ist grundsätzlich in einem englischen Wörterbuch folgendermaßen definiert:
„Compliance /kəmplaiəns/ noun [U] ~ (with sth) the practice of obeying rules or requests made by people in authority: procedures that must be followed to ensure full compliance with the law ◊ Safety measures were carried out in compliance with paragraph 6 of the building regulations. NON-COMPLIANCE – see also COMPLY” (Hornby 2007, S. 309).

Diese Definition ist sehr eng gefasst, denn Compliance bezieht sich hier ausschließlich auf die Befolgung von Regeln bzw. Gesetzen, verfasst von Behörden. Eine ähnlich stark simplifizierte, aber grundlegende Begriffsbestimmung nimmt HAUSCHKA vor. Danach bedeutet Compliance ohne konkreten Bezugsrahmen in etwa „Befolgung, Übereinstimmung, Einhaltung von bestimmten Geboten“, d. h. Unternehmen und Organe müssen sich innerhalb geltender Rechtsnormen und -vorschriften bewegen (Hauschka 2007a, S. 2).

Neben dem allgemeinen Compliance-Begriff, der sich generalistisch auf jeden (Funktions-) Bereich einer Organisation anwenden lässt, hat sich der Ausdruck IT-Compliance speziell für den Bereich der Informationstechnologie etabliert. Dies ist insbesondere auf den enormen Bedeutungszuwachs der IT für Unternehmen in den letzten 10 Jahren und der damit verbundenen Notwendigkeit der Berücksichtigung der IT in Gesetzen und Regularien zurückzuführen.

KLOTZ bezeichnet IT-Compliance als „einen Zustand, in dem alle für die IT des Unternehmens relevanten Vorgaben nachweislich eingehalten werden“ (Klotz 2009, S. 6). Dabei sind ausdrücklich alle IT-Leistungen, also sowohl unternehmensinterne als auch -externe (z. B. im Rahmen von Outsourcing), zu berücksichtigen (Klotz 2009, S. 6).

Welche Vorgaben als relevant angesehen werden bzw. auf welche Art diese klassifiziert werden können, verdeutlicht nachfolgende Abbildung.

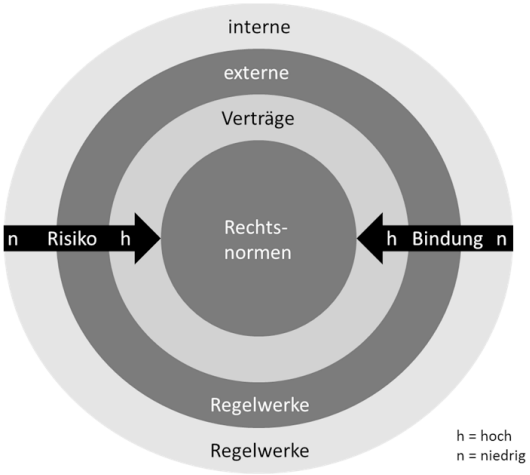

Abb. D-1: Zwiebelmodell für Compliance-relevante Regelwerke (Klotz und Dorn 2008, S. 11)

- **Rechtsnormen** (z. B. Signaturgesetz (SigG), Bundesdatenschutzgesetz (BDSG), Telemediengesetz (TMG), 8. EU-Richtlinie)
- **Verträge** (z. B. Kontrakte und Vereinbarungen mit Kunden, Lieferanten, sonstigen Marktteilnehmern)
- **Externe Regelwerke** (z. B. IT-Grundschutz, ISO/IEC 27001/2, IT Infrastructure Library (ITIL), Control Objectives for Information and related Technology (CobiT))
- **Interne Regelwerke** (z. B. Verfahrensanweisungen, Regelungen, Richtlinien, Service Level Agreements (SLAs))

Im Vergleich zu den drei anderen Kategorien ist der Bindungsgrad und das Risiko bei den Rechtsnormen am höchsten, da geltende Gesetze und Rechtsverordnungen ohne Ausnahmen oder Wahlmöglichkeiten von allen, die adressiert werden, unbedingt einzuhalten sind. Die internen Regelwerke sind hingegen nur für dasjenige Unternehmen relevant, welches diese Richtlinien verfasst hat und freiwillig einhält. Daher weisen unternehmensinterne Regelwerke den niedrigsten Bindungsgrad und das geringste Risiko auf. (Klotz 2009, S. 20)

GAULKE definiert IT-Compliance in einer sehr ähnlichen Art und Weise, da auch hier eine Differenzierung nach relevanten Gesetzen und Rechtsverordnungen, vertraglichen Verpflichtungen sowie externen und internen Richtlinien erfolgt. Jedoch wird in dieser Begriffsbestimmung der Aspekt der nachweislichen Einhaltung noch genauer konkretisiert. So sind von einer Organisation Prozesse einzurichten, welche nicht nur die Einhaltung der relevanten Bestimmungen überwachen, sondern auch Nachweise für die Konformität gegenüber internen und externen Interessensgruppen erbringen. (Gaulke 2010, S. 183)

Norm, Standard und IT-Framework

Grundsätzlich lassen sich unter dem Begriff „Standard“ die Ausdrücke „Norm“, „Industrie-Standard“, „De-facto-Standard“ und „herstellerspezifischer Standard“ subsumieren, je nachdem auf welcher Grundlage und auf welchem Entwicklungsprozess der Standard beruht.

Eine Norm ist definiert als „Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird" (DIN Deutsches Institut für Normung e. V. 2007, S. 25). Entscheidend ist hier die Tatsache, dass dieses Dokument in

festgelegten Prozessen innerhalb einer Normierungsorganisation wie z. B. DIN oder ISO entstanden ist.

Ein Industrie-Standard bzw. De-facto-Standard ist ein Regelwerk, eine Spezifikation oder eine Verfahrensweise, welche ohne ein Normierungsverfahren entstanden ist, sondern im Laufe der Zeit durch die Praxis in Form von Anwendern und Herstellern für eine bestimmte Problemstellung entwickelt wurde und durch häufigen Gebrauch in der Alltagswelt wie eine echte Norm angesehen werden kann (Schubert 2008, S. 71).

Ein herstellerspezifischer Standard ist dann gegeben, wenn eine Vielzahl von Anwendern aufgrund mehrjähriger Erfahrungen die Erkenntnis gewinnt, dass es vorteilhaft ist, den firmenspezifischen Spezifikationen eines Herstellers zu folgen (Schubert 2008, S. 70-71).

Der Begriff „IT-Framework“ wird weder in der Wissenschaft noch in der Praxis trennscharf verwendet. Ursprünglich kommt die Bezeichnung aus der Softwareentwicklung, diese findet jedoch zunehmend auf Methoden und Vorgehensweisen des IT-Managements Anwendung. Im englischen Sprachgebrauch wird oftmals das Wort „Framework“ als Synonym für Norm, Standard oder Methodik gebraucht. VAN BON und VERHEIJEN bezeichnen beispielsweise ISO/IEC 9000, ISO/IEC 27001, CobiT und ITIL als Frameworks (van Bon und Verheijen 2006). Auch die Autoren von CobiT verwenden den Begriff „IT-Framework“, obwohl in diesem Fall auch die Bezeichnung „De-facto-Standard“ zutreffen würde, da CobiT als das Referenzmodell für IT-Governance angesehen wird.

15.2.2 Ausgewählter Überblick über branchenunspezifische IT-Compliance-Anforderungen

Auf Basis der Erläuterung des Begriffs IT-Compliance im vorherigen Abschnitt wird in diesem Abschnitt ein Auszug von generellen rechtlichen und regulatorischen Anforderungen an die IT dargestellt, um den Begriff IT-Compliance inhaltlich beispielhaft zu konkretisieren.

Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) wurde in der ursprünglichen Fassung am 27.01.1977 im Bundesgesetzblatt veröffentlicht und am 01.01.1978 offiziell in Kraft gesetzt, wobei dieses im Laufe der Zeit durch den Gesetzgeber an die aktuellen Gegebenheiten immer wieder angepasst wurde. Das BDSG regelt neben den Datenschutzgesetzen der einzelnen Bundesländer den Umgang (Erhebung, Ver-

arbeitung und Nutzung) mit personenbezogenen Daten, die manuell oder in IT-Systemen verarbeitet werden, denn nach § 1 Abs. 1 BDSG besteht der Zweck des Gesetzes darin, „den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (Bundesdatenschutzgesetz 2009).

Die Verdeutlichung der rechtlichen Anforderungen an die IT erfolgt exemplarisch anhand des § 9 Satz 1 BDSG. Dieser Paragraph besagt, dass „öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen [haben], die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten“ (Bundesdatenschutzgesetz 2009). Dabei werden in der Anlage zu § 9 Satz 1 BDSG acht Kontrollmaßnahmen aufgeführt, die von GOLA und SCHOMERUS mit Beispielen unterlegt werden (Gola und Schomerus 2010, S. 356-358):

- **Zutrittskontrolle** (z. B. durch Chipkarten/Transponderkarten, Alarmanlagen, Videotechnik)
- **Zugangskontrolle** (z. B. durch Protokollierung der Passwortnutzung, Passwortvergabe)
- **Zugriffskontrolle** (z. B. durch automatische Prüfung der Zugriffsberechtigung, Protokollierung der Systemnutzung)
- **Weitergabekontrolle** (z. B. durch Datenverschlüsselung, Vollständigkeits- und Richtigkeitsprüfung)
- **Eingabekontrolle** (z. B. durch Protokollierung eingegebener Daten, Verarbeitungsprotokolle)
- **Auftragskontrolle** (z. B. durch Maßnahmen zur Aufbewahrung und bei Verlust von Datenträgern)
- **Verfügbarkeitskontrolle** (z. B. durch Auslagerung von Sicherungskopien, Vorhandensein von Katastrophenplänen)
- **Trennungsgebots** (z. B. durch Zugriffregelung, Mandantentrennung, Dateiseparierung bei Datenbankprinzip)

Die Auflistung der acht Kontrollmaßnahmen sowie die entsprechend dazu aufgeführten Beispiele verdeutlichen, wie stark die IT im Kontext des § 9 BDSG adressiert wird.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Vor dem Hintergrund zahlreicher Unternehmenskrisen, der zunehmenden Globalisierung der Aktionärsstrukturen und der wachsenden Internationalisierung der Kapitalmärkte in Verbindung mit der Forderung der internationalen Vergleichbarkeit trat im Mai 1998 das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in Kraft (Schuppener und Tillmann 1999, S. 20). Als Artikelgesetz verändert bzw. ergänzt es bestehende Gesetze wie das Aktiengesetz (AktG) und das Handelsgesetzbuch (HGB). Das KonTraG verfolgt insbesondere zwei Ziele (Speichert 2007, S. 245):

- Korrektur von Verhaltensfehlsteuerungen und Schwächen im deutschen Unternehmenskontrollsystem des Aktienrechts und des Mitbestimmungsrechts
- Berücksichtigung der steigenden Ausrichtung deutscher Publikumsgesellschaften am Informationsbedarf internationaler Investoren

An Hand der folgenden Auszüge aus dem KonTraG lassen sich entsprechende Implikationen für die IT verdeutlichen.

§ 91 AktG wurde um einen neuen Absatz erweitert, der lautet:
„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Durch diese Erweiterung des § 91 AktG wird ausdrücklich betont, dass der Vorstand verpflichtet ist, ein angemessenes und funktionierendes Risikomanagement zu etablieren. Da mittlerweile nahezu alle Geschäftsprozesse in einem Unternehmen durch IT unterstützt werden, sind mit dem IT-Einsatz auch entsprechende Risiken verbunden, die im Rahmen eines (IT-) Risikomanagements identifiziert, bewertet, gegebenenfalls minimiert und kontrolliert werden müssen. Somit wird deutlich, dass diese gesetzliche Neuregelung auch direkt die IT betrifft.

Das GmbHG wurde nicht explizit um eine solche Bestimmung erweitert, da laut der Gesetzesbegründung davon auszugehen ist, dass die Änderung des Aktiengesetzes auch eine Ausstrahlungswirkung auf GmbHs haben wird, welche in Größe, Komplexität und Struktur mit einer AG vergleichbar sind (Deutscher Bundestag 1998, S. 15).

Bezogen auf § 91 Abs. 2 AktG wurde auch der Prüfungsumfang des Abschlussprüfers dementsprechend angepasst. Dies erfolgte in § 317 Abs. 4 HGB:

„Bei einer Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91 Abs. 2 des Aktiengesetzes obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Da ein Überwachungssystem (in Form eines Risikomanagements) zum einen heutzutage häufig mit Hilfe von IT realisiert wird und zum anderen die IT als geschäftskritischen Faktor überwacht, sind die Auswirkungen dieser Neuregelung, auch bezogen auf die Interpretation von § 91 Abs. 2 AktG, auf die IT offensichtlich.

Als letzter Auszug werden die Änderungen von § 289 Abs. 1 HGB und § 315 Abs. 1 HGB erläutert. Die beiden Paragraphen wurden jeweils um folgenden Teilsatz erweitert: „dabei ist auch auf die Risiken der künftigen Entwicklungen einzugehen“ (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich 1998).

Der Hintergrund dieser gesetzlichen Neuregelung liegt in der Tatsache begründet, dass Unternehmen nicht selten in eine Krise geraten sind oder Insolvenz anmelden mussten, obwohl sie kurz vorher vom Abschlussprüfer eine uneingeschränkte Bestätigung ihres Jahresabschluss- und Lageberichts erhalten hatten, wobei formalrechtlich dem Prüfer kein Vorwurf gemacht werden konnte. Um diesem Umstand zu begegnen ist der Lagebericht um einen Risikobericht zu ergänzen, in welchem die Unsicherheiten der künftigen Entwicklung dargestellt werden. Da die mit dem IT-Einsatz verbundenen Risiken durchaus einen bestandsgefährdenden Charakter einnehmen können, sind diese im Risikobericht zu erfassen. (Speichert 2007, S. 245; Bertele und Lehner 2008, S. 11)

15.2.3 Konsequenzen bei Nichteinhaltung der IT-Compliance

Nach der Erläuterung des Begriffs IT-Compliance und der anschließenden konkreten Darstellung einiger IT-relevanter Compliance-Vorschriften muss der Frage nachgegangen werden, welche Auswirkungen die Nichteinhaltung von Gesetzen und Regularien nach sich ziehen können. Da jedoch eine trennscharfe Unterscheidung zwischen Konsequenzen aus IT-Compliance-Verstößen und Folgen aufgrund anderweitiger Compliance-Verletzungen nicht sinnvoll bzw. möglich ist, wird an dieser Stelle die Betrachtung auf die ganzheitliche Compliance erweitert.

Die Frage nach möglichen Auswirkungen wird unter anderem in der aktuellen Studie „The True Cost of Compliance“ beantwortet, welche durch das PONEMON INSTITUT in Zusammenarbeit mit dem Unternehmen Tripwire entstand (Ponemon Institute 2011). Dabei wurden 160 Führungsverantwortliche aus 46 multinationalen Unternehmen befragt. Ein wesentliches Ergebnis zeigt auf, dass die durchschnittlichen Kosten für ein Unternehmen für die dauerhafte Einhaltung der geltenden Compliance-Vorschriften bei circa 3,5 Mio. US-Dollar (2,5 Mio. Euro) liegen, wohingegen die Verletzung bzw. die Nichteinhaltung von Compliance-Regelungen (z. B. Gesetze, Regularien, Verträge, Richtlinien) zu durchschnittlichen Kosten in Höhe von etwa 9,4 Mio. US-Dollar (6,7 Mio. Euro) pro Unternehmen führen (siehe Abb. D-2). Zusammengefasst lässt sich damit festhalten, dass eine „Vernachlässigung“ des Compliance-Managements inklusive der daraus resultierenden Konsequenzen 2,65-mal höhere Kosten verursacht als ein effektives und effizientes Compliance-Management ohne Verstöße. Damit wird auch die Aussage der folgenden aus dem amerikanischen Raum stammenden Redewendung belegt: „If you think compliance is expensive, try non-compliance.“

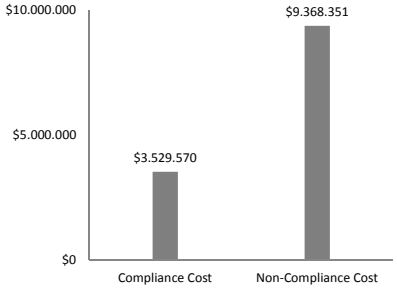

Abb. D-2: Durchschnittliche Kosten für Einhaltung und Nichteinhaltung der IT-Compliance
(Ponemon Institute 2011, S. 5)

Neben Schadensersatzansprüchen, Bußgeldern oder Kompensationszahlungen als mögliche Konsequenzen von Compliance-Verstößen ist eine detaillierte Auflistung von möglichen Kosten bei OHRTMANN zu finden (Ohrtmann 2009, S. 71). Diese liefert eine plausible Begründung für die deutlich höheren Kosten bei Nichteinhaltung von Compliance-Regelungen.

15.2.4 Probleme bei der Umsetzung bzw. Einhaltung von IT-Compliance-Anforderungen

Unternehmen stehen bei der Einhaltung von rechtlichen und regulatorischen IT-Anforderungen vor einigen Herausforderungen, die es zu bewältigen gilt. Zum einen steigt die Anzahl der zu erfüllenden IT-Compliance-Vorschriften kontinuierlich an, was den Unternehmen zunehmend „Kopfzerbrechen“ bereitet. Dies belegt auch eine Studie von GMG Insight, die zu dem Schluss gelangt, dass „the heavy burden of regulatory compliance is a truly global issue” (Trub und Olski 2008, S. 5).

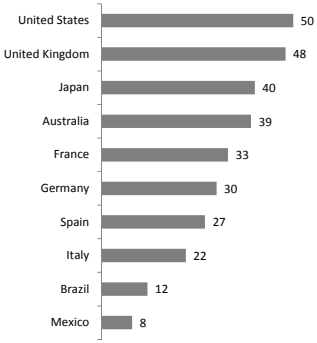

Abb. D-3: Anzahl an vorgeschriebenen, separaten gesetzlichen Regulierungen nach Ländern (Mittelwerte)
(Trub und Olski 2008, S. 5)

Alleine für Deutschland wurden 30 IT-Compliance-Anforderungen identifiziert, die für ein Unternehmen relevant sein können (siehe Abb. D-3). Vor allem die permanente, nachweisliche Einhaltung gestaltet sich aufgrund der Menge als äußerst schwierig.

Zum anderen ist bezogen auf ein Unternehmen eine Vielzahl an Gruppen und Funktionen an der Herstellung von IT-Compliance Konformität beteiligt, wie Abb. D-4 verdeutlicht. Diese heterogenen Einheiten hinsichtlich der Einhaltung rechtlicher und regulatorischer IT-Anforderungen zu steuern, abzustimmen und zu kontrollieren stellt eine weitere große Herausforderung dar.

Abb. D-4: An IT-Compliance beteiligte Gruppen und Funktionen (Klotz 2009, S. 13)

Ein weiteres Problem liegt vermehrt in der eigentlichen Umsetzung der IT-Compliance-Anforderungen, da sowohl der Gesetzgeber als auch die Aufsichtsorgane zunehmend eine Abkehr von der traditionell Regel-basierten Aufsicht hin zu einer Prinzipien-basierten Aufsicht vollziehen, d. h. den Unternehmen wird in Form von sehr generalistisch gehaltenen Empfehlungen bzw. Handlungsanweisungen bewusst mehr Gestaltungsspielraum für die Erfüllung der entsprechenden Gesetze und Regularien gegeben (Bretz et al. 2007, S. 3). Dies sollte eigentlich im Interesse der Unternehmen sein, jedoch herrscht oftmals eine gewisse Unsicherheit vor, ob die entsprechende Anforderung tatsächlich korrekt im Sinne des Verfassers umgesetzt wurde.

Werden diese Probleme zusätzlich im organisationsübergreifenden Kontext gesehen sowie Hochflexibilität zugrunde gelegt, dann sind die Herausforderungen nicht mehr isoliert auf ein Unternehmen beschränkt, sondern müssen in einer sich dynamisch verändernden Umgebung betrachtet werden. Gerade die unvollständige Planbarkeit sowie die Überlappung von Planung und Ausführung als Eigenschaften von hGP in Verbindung mit einer Vielzahl von Prozessteilnehmern führen zu dem Umstand, dass die zuvor beschriebenen Herausforderungen noch an deutlicher Komplexität und Vielschichtigkeit gewinnen. Insbesondere der Grundsatz „Eine Kette ist nur so stark wie ihr schwächstes Glied“ verdeutlicht die Gesamtproblematik.

15.3 Anforderungen an Standards/IT-Frameworks im Kontext hochflexibler Geschäftsprozesse

In diesem Abschnitt erfolgt die Aufstellung eines Anforderungskatalogs, welcher im späteren Verlauf zur Eignungsanalyse auf die in Abschnitt 15.4 dargestellten Standards/IT-Frameworks angewendet wird. In diesem Zusammenhang wird auch deutlich gemacht, welche Kriterien für hGP besonders wichtig sind. Folgende Anforderungen wurden identifiziert:

- Die **Verbreitung** zeigt auf, welche geographische Ausrichtung bei dem entsprechenden Standard/IT-Framework gegeben ist. Bezogen auf hGP ist generell eine eher internationale Orientierung zu bevorzugen. Dies ist jedoch insbesondere unter dem Aspekt der Globalisierung zu sehen.
- Die **Vollständigkeit** verdeutlicht, in welchem Ausmaß ein Standard/IT-Framework verschiedene Facetten (z. B. Metriken, Verantwortlichkeiten, Reifegradmodell, etc.) beinhaltet. Für den Kontext hGP ist dieses Kriterium nicht spezifisch, jedoch bietet eine größere Vielfalt grundsätzlich mehr Handlungsspielraum.
- Der Aspekt **Transparenz** liefert eine Aussage über den Detailierungsgrad der Inhalte eines Standards/IT-Frameworks sowie über die Klarheit der Formulierungen. Für hGP stellt dies kein spezielles Kriterium dar, jedoch ist grundsätzlich eine hohe Detailtiefe vorteilhaft.
- Unter **Elastizität** ist die Fähigkeit zu verstehen, wie gut einzelne Elemente aus einem Standard/IT-Framework herausgelöst und anschließend separat verwendet werden können. Diese Anforderung ist für hGP besonders wichtig, da je nach vorliegender Situation (welche Daten werden an wen weitergegeben bzw. von wem weiterverarbeitet) ein angemessenes Compliance-Niveau auf unterschiedlich stark bzw. schwach formulierten Regelungen beruht.
- Das Vorhandensein eines **Reifegradmodells** ist eine weiteres Kriterium, welches aufzeigen soll inwiefern ein Standard/IT-Framework die Option enthält, einzelne inhaltliche Anforderungen in unterschiedlich starken bzw. schwachen Auslegungen zur flexiblen Steuerung der Ausprägung von „Compliance-Konformität“ auszugestalten. Im Kontext von hGP ist dieser Aspekt von besonderer Wichtigkeit, da vor allem im organisationsübergreifenden Zusammenhang Informationen mit unterschiedlichem Schutzbedarf empfangen, verarbeitet und weitergegeben werden. Dabei ist bei der Ausgestaltung der entsprechenden Absicherungsmaßnahmen

der Grundsatz der Verhältnismäßigkeit zu beachten.

- Unter **Auditierbarkeit** ist zu verstehen, wie nachvollziehbar und eindeutig die Umsetzung der Inhalte eines Standards/IT-Frameworks überprüfbar ist. Dies ist abhängig davon, wie klar, detailliert und unmissverständlich ein Standard/IT-Framework formuliert ist. Denn je unschärfer und generalistischer die Inhalte verfasst sind, desto mehr Interpretations- und Gestaltungsspielraum ist den Unternehmen bei der Umsetzung gegeben und umso schwieriger gestaltet sich die Überprüfung (z. B. durch Interne Revision oder Wirtschaftsprüfungsunternehmen), ob die gestellte Anforderung von einem Unternehmen erfüllt wird. Dieses Kriterium ist in Bezug auf hGP von zentraler Bedeutung, da aufgrund der Eigenschaften unvollständige Planbarkeit und Überlappung von Planung und Ausführung möglichst konkrete Handlungs- bzw. Umsetzungsanweisungen vorteilhaft sind.
- Die unvollständige Planbarkeit sowie die Überlappung von Planung und Ausführung als hGP-Eigenschaften erfordern schnelle Aussagen darüber, ob das Unternehmen, welches den nächsten Teilprozess ausführen will und daher entsprechende Informationen vom Vorgänger benötigt, die gestellten IT-Compliance-Anforderungen erfüllt. Diese ad-hoc Aussagen lassen sich nur mit einer geeigneten **Werkzeug-Unterstützung** realisieren. Im hGP-Kontext ist diese Anforderung daher von zentraler Bedeutung.

15.4 Standards/IT-Frameworks, die für hGP in Frage kommen

Wie in Abschnitt 15.2.4 dargestellt, sind die Umsetzung von IT-Compliance-Anforderungen und deren nachweisliche Einhaltung mit einer Reihe von Problemen bzw. Herausforderungen verbunden. Diesen Schwierigkeiten lässt sich mit der Anwendung von Standards/IT-Frameworks begegnen. Jene können in folgenden Fällen besonders hilfreich sein:

- bei der Konkretisierung von Gesetzen und Regularien hin zu umsetzbaren Anweisungen
- bei der Erhöhung der Transparenz der Qualität der jeweiligen internen IT-Compliance-Regelungen
- bei der Setzung von konkreten „Leitplanken“ trotz unvollständiger Planbarkeit als Eigenschaft von hGP

Zu diesem Zweck werden nachfolgend vier ausgesuchte Standards bzw. IT-Frameworks erläutert, welche für den hGP-Kontext als geeignet erscheinen.

15.4.1 IT-Grundschutz

Der IT-Grundschutz ist eine Methodik des Bundesamtes für Sicherheit in der Informationstechnik (BSI), welche eine strukturierte Vorgehensweise für das Management der Informationssicherheit liefert. Es handelt sich dabei um einen ganzheitlichen Sicherheitsansatz, welcher alle relevanten Bereiche und Aspekte der Informationssicherheit berücksichtigt (Speichert 2007, S. 262). Im Jahr 1994 wurde erstmalig diese Methode unter dem Namen „IT-Grundschutzhandbuch“ vom BSI veröffentlicht. Dieses wurde im Laufe der Zeit kontinuierlich in Form von Ergänzungslieferungen aktualisiert. Als Resultat der Neustrukturierung des IT-Grundschutzhandbuchs im Jahr 2005 wurden die IT-Grundschutz-Standards und die IT-Grundschutzkataloge geschaffen.

Die IT-Grundschutz-Standards beinhalten Empfehlungen zu Methoden, Prozessen, Verfahren, Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Folgende Standards wurden bis dato vom BSI veröffentlicht:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

Die IT-Grundschutz-Kataloge sind vollständig modular aufgebaut. Die Bausteine „spiegeln typische Abläufe von Geschäftsprozessen und Bereiche des IT-Einsatzes wider“ (Bundesamt für Sicherheit in der Informationstechnik 2009, S. 17). Für jeden Baustein sind entsprechende Gefährdungen beschrieben, welchen wiederum durch definierte Maßnahmen begegnet werden kann.

15.4.2 ISO/IEC 27002

Der von der International Organization for Standardization (ISO) herausgegebene Standard (bzw. Norm) ISO/IEC 27002 mit dem Titel „Information technology – Security techniques – Code of practice for information security management“ beinhaltet eine Sammlung von (Best Practice) Maßnahmen, Verfahren und Methoden zur Herstellung bzw. Wahrung der Informationssicherheit.

Der Standard basiert auf dem British Standard BS 7799-1, welcher 1995 erstmalig veröffentlicht wurde. Die ISO übernahm den Standard mit unverändertem Inhalt und publizierte diesen im Jahr 2000 unter der Bezeichnung ISO/IEC

17799. Im Jahr 2005 erfolgte die Umbenennung in ISO/IEC 27002 und die Zuordnung zur Normenreihe ISO/IEC 27000.

Dieser Standard „establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" (International Organization for Standardization 2005, S. 1) und stellt somit eine Art Leitfaden für das Management der Informationssicherheit dar. Zudem dient die Norm dem besseren Verständnis der in ISO/IEC 27001 definierten Anforderungen und ist als Ausgangslage zur Entwicklung von unternehmensindividuellen Regelungen und Richtlinien gedacht.

Im ISO/IEC 27002 werden 11 Bereiche betreffend der Informationssicherheit (Security Control Clauses) adressiert, welche zusammen 39 Sicherheitskategorien (Security Categories) enthalten. Jede dieser Kategorien setzt sich aus einer Zielvorgabe (Control Objective) und einer oder mehrerer Maßnahmen (Controls) zusammen. Eine Maßnahme besteht wiederum aus einem Umsetzungsleitfaden (Implementation Guidance) und optionalen weiteren Informationen (Other Information). (International Organization for Standardization 2005)

15.4.3 IT Infrastructure Library

Um das Jahr 1990 wurde die IT Infrastructure Library (ITIL) durch die damalige Central Computer and Telecommunications Agency (CCTA) im Auftrag der britischen Regierung entwickelt, mit dem Ziel einen offenen Standard für das IT-Service-Management zu entwerfen (Rudd 2006, S. 149). Seit 2001 obliegt die kontinuierliche Weiterentwicklung von ITIL beim Office of Government Commerce (OGC), da das CCTA in das OGC integriert wurde. ITIL ist eine Sammlung von Best Practices und hat sich mittlerweile als De-facto-Standard im IT-Service-Management etabliert.

Im Jahr 2007 wurde die bis dato letzte Aktualisierung vorgenommen und ITIL in Version 3 (ITIL v3) veröffentlicht. Kennzeichnend für die neue Fassung sind die stärkere Ausrichtung an den Geschäftsanforderungen (IT-Business-Alignment) und die Fokussierung auf einen Service-Lebenszyklus.

ITIL v3 bietet „a unique set of guidelines that creates a view of how mature IT organizations should provide effective business service management (BSM)" (Shuja 2011, S. 45). Weiter ermöglicht ITIL v3 „IT organizations to plan and implement their transformations and improvements to achieve BSM" (Shuja 2011, S. 45). Die Kernpublikation von ITIL v3 besteht aus den folgenden fünf Büchern (Office of Government Commerce 2007b):

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Jedes dieser Bücher deckt einen Bereich des Service-Lebenszyklus ab (siehe Office of Government Commerce 2007a).

15.4.4 Control Objectives for Information and Related Technology

Das IT-Framework „Control Objectives for Information and Related Technology" (CobiT) wurde in der ersten Version im Jahr 1996 von der Information Systems Audit and Control Association (ISACA) veröffentlicht. Seit 1998 obliegt die kontinuierliche Weiterentwicklung von CobiT dem IT Governance Institut, welches von der ISACA gegründet wurde. Aktuell liegt das IT-Rahmenwerk in der Version 4.1 vor.

Die allgemeine Intension von CobiT lautet:
„To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals" (IT Governance Institute 2007, S. 9).

Durch die Anwendung von CobiT lassen sich folgende konkrete Zielsetzungen erreichen (Johannsen und Goeken 2007, S. 41):

- Ausrichtung der IT-Planungen an den geschäftlichen Anforderungen
- Organisation der IT-Aktivitäten durch ein allgemein akzeptiertes Modell
- Unterstützung der ökonomischen Verwendung von IT-Ressourcen
- Bereitstellung von IT-relevanten Steuerungs- und Managementinformationen durch Kontrollelemente

CobiT beinhaltet ein Prozessmodell von international akzeptierten IT-prozessbezogenen Kontrollzielen (Control Objectives), welche in einem Unternehmen beachtet und umgesetzt werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten (Sewera 2005, S. 20). Denn erst wenn die Organisation der Informationen, Anwendungen, Infrastruktur und Menschen richtig funktioniert, werden die Geschäftsprozesse die an sie gestellten Anforderungen erfüllen (Gaulke 2010, S. 10).

Die Erreichung der vorgegebenen Ziele (Geschäftsanforderungen) wird durch IT-Prozesse unter Einbeziehung von IT-Ressourcen realisiert.

Die IT-Ressourcen müssen geplant, entwickelt, implementiert, betrieben und überwacht werden. Hierfür sind in CobiT in der aktuellen Fassung insgesamt 34 kritische IT-Prozesse definiert, welche erfolgsbestimmend für das Management der IT sind (Bitterli 2006, S. 18). Jeder dieser IT-Prozesse ist jeweils zu einem der nachfolgend aufgelisteten Bereiche bzw. einer Domäne zugeordnet:

- Planen und Organisieren (Plan and Organise, PO)
- Beschaffen und Implementieren (Acquire and Implement, AI)
- Erbringen und Unterstützen (Deliver and Support, DS)
- Überwachen und Beurteilen (Monitor and Evaluate, ME)

Die Einteilung in diese Domänen basiert auf dem Lebenszyklus von IT-Systemen (Design, Build, Run und Monitor) (Johannsen und Goeken 2007, S. 60).

Jeder der 34 IT-Prozesse ist gleich strukturiert. Die Komponenten werden im Folgenden erläutert:

- Die **Prozessbeschreibung** (Process Description) enthält die jeweiligen Prozessziele, die betroffenen IT-Ressourcen, die betroffenen primären und sekundären Informationskriterien sowie in einer wasserfallähnlichen Darstellung die wichtigsten Geschäftsziele für die IT, IT-Ziele, Kontrollen und Metriken.
- Zwischen drei und 15 **Kontrollziele** (Control Objectives) sind für jeden Prozess definiert und konkretisieren die Ziele aus der Prozessbeschreibung.
- Die **Leitlinien für das Management** (Management Guidelines) bestehen aus folgenden drei Elementen:
    1. Prozesseingangs- und -ausgangswerte (Inputs/Outputs)
    2. Kompetenzmatrix (RACI Chart)
    3. Ziele und Metriken (Goals and Metrics)

Das **Reifegradmodell** (Maturity Model) von CobiT basiert auf dem Reifegradmodell des Capability Maturity Model Integration (CMMI) (vgl. www.sei.cmu.edu/cmmi) des Software Engineering Institutes. Es beschreibt den Reifegrad für jeden Prozess in sechs Abstufungen (nicht existent, initial, wiederholbar, definiert, gesteuert und überwacht, optimiert).

15.5 Bewertung

Im folgenden Abschnitt erfolgt nun die Bewertung der zuvor dargestellten Standards bzw. IT-Frameworks anhand der in Abschnitt 15.3 spezifizierten Anforderungen. Dabei ist jedoch zu beachten, dass diese Standards/IT-Frameworks teilweise verschiedene Themenbereiche sowie Schwerpunkte adressieren und somit der Umfang der behandelten Aspekte durchaus schwankt (Informationssicherheit beispielsweise wird von allen vier Standards/IT-Frameworks in unterschiedlichen Ausprägungen behandelt). IT-Grundschutz und ISO/IEC 27002 sind Standards für das Management der Informationssicherheit, ITIL stellt eine Best Practice Sammlung für das IT-Service-Management dar und CobiT ist ein Framework für die IT-Governance. Daher wird bei der Bewertung nicht der fachliche Schwerpunkt zugrunde gelegt, sondern der Fokus liegt auf der Struktur und der gesamten Handhabbarkeit, denn nur auf diese Weise ist eine Vergleichbarkeit gegeben.

Die nachfolgende Darstellung verdeutlicht das Ergebnis der durchgeführten Bewertung der vier genannten Standards/IT-Frameworks (siehe Abb. D-5). Die genaueren Erläuterungen hinsichtlich der einzelnen Bewertungen erfolgen im Anschluss an die kommende Abbildung.

	Standards/IT-Frameworks	IT-Grundschutz	ISO/IEC 27002	ITIL	CobiT
Kriterien	Verbreitung	-	+	+	+
	Vollständigkeit	+	-	o	+
	Transparenz	+	o	o	+
	Elastizität *	+	+	+	o
	Reifegradmodell *	-	-	-	+
	Auditierbarkeit *	+	o	o	+
	Werkzeug-Unterstützung *	+	+	+	o

* besonders relevant für hGP

- = negative, o = neutrale, + = positive Bewertung

Abb. D-5: Analyse der Standards/IT-Frameworks

Bezüglich der **Verbreitung** finden ISO/IEC 27002, ITIL und CobiT international deutlich mehr Anklang als IT-Grundschutz. Dies liegt vor allem daran, dass im Gegensatz zu IT-Grundschutz bei den anderen drei Standards/IT-Frameworks entweder eine internationale Normierung (durch die ISO) stattfand und/oder

deren Entwicklung durch einen global ausgerichteten Verband erfolgte. Auch die Sprache, in der ein Standard/IT-Framework (ursprünglich) verfasst bzw. veröffentlicht wurde, ist ein wichtiger Faktor (IT-Grundschutz in Deutsch, alle anderen in Englisch).

Die **Vollständigkeit** ist bei IT-Grundschutz und bei CobiT am besten ausgeprägt, da diese im Vergleich zu den anderen Standards/IT-Frameworks die meisten Facetten (Metriken, Verantwortlichkeiten, Reifegradmodell, Vorgehensweisen, etc.) enthalten. Am schlechtesten schneidet bei diesem Kriterium ISO/IEC 27002 ab.

Bei IT-Grundschutz und CobiT besteht im Vergleich zu ISO/IEC 27002 und ITIL eine höhere **Transparenz**, insbesondere hinsichtlich Klarheit und Eindeutigkeit der formulierten Inhalte.

Bezogen auf die **Elastizität** ist CobiT nur eingeschränkt zu empfehlen, da die Prozesse aufgrund von definierten In- und Outputs untereinander verbunden sind. Somit sind diese Verknüpfungen nur bedingt nutzbar, falls einzelne Prozesse herausgelöst aus dem gesamten IT-Framework angewendet werden. Bei den anderen drei betrachteten Standards/IT-Frameworks lassen sich einzelne Elemente weitestgehend ohne „hinderliche“ Abhängigkeiten separat einsetzen.

Ein **Reifegradmodell** zur Abstufung von entsprechenden fachlichen Inhalten enthält nur CobiT. IT-Grundschutz, ISO/IEC 27002 und ITIL enthalten kein derartiges Element.

Die **Auditierbarkeit** des IT-Grundschutz ist positiv zu bewerten, da speziell die Maßnahmen (als Teilbereich der IT-Grundschutz-Kataloge) ergänzende Kontrollfragen beinhalten, welche zudem im Laufe der kontinuierlichen Weiterentwicklung sukzessive durch Prüffragen ersetzt werden. Da CobiT von der ISACA, dem Verband der IT-Auditoren und IT-Revisoren, entwickelt wurde, enthält dieser ebenso entsprechende Prüfungselemente, weshalb auch hier die Analyse zu einem positiven Ergebnis hinsichtlich der Auditierbarkeit führt. Im Gegensatz dazu sind ISO/IEC 27002 und ITIL nicht explizit für Prüfungen (Audits) konzipiert worden und daher lassen sich diese nur in eingeschränktem Maße (z. B. als Grundlage für Prüfungspunkte) hierfür verwenden.

Hinsichtlich der **Werkzeug-Unterstützung** hat die Analyse gezeigt, dass für IT-Grundschutz, ISO/IEC 27002 und ITIL sehr viele Lösungen auf dem Markt vorhanden sind. Im Vergleich dazu ist bei CobiT das Angebot an Softwareprodukten eher eingeschränkt. Dies könnte vermutlich in der Tatsache begründet sein, dass CobiT sehr komplexe Strukturen und Abhängigkeiten beinhaltet.

Abb. D-5 und die anschließenden Erläuterungen zeigen, dass CobiT am besten die gestellten Anforderungen erfüllt. Schwächen sind nur bezüglich der Kriterien Elastizität und Werkzeug-Unterstützung vorhanden. Auf den nächsten Plätzen folgen IT-Grundschutz und ITIL, ISO/IEC 27002 belegt den letzten Rang.

Durch die unvollständige Planbarkeit als hGP-Eigenschaft kann jedoch wie eingangs erwähnt nicht vorgeschrieben werden, dass jeder Teilnehmer in einem sich ad-hoc bildenden Wertschöpfungsnetz den gleichen Standard bzw. das gleiche IT-Frameworks verwendet. Daher ist die Frage zu beantworten, wie die Situation zu behandeln ist, wenn andere Standards/IT-Frameworks bei potenziellen Teilnehmern im Einsatz sind und deren Partizipation am Wertschöpfungsnetz nicht von vorneherein ausgeschlossen werden soll.

Dieser Problemstellung lässt sich zunächst mit Hilfe von sogenannten Mapping-Tabellen begegnen. Gegenstand der Tabellen ist die Darstellung von inhaltlichen Überschneidungen zwischen Standards/IT-Frameworks. Damit wird die Möglichkeit geschaffen, dass auch durch die Verwendung eines anderen Standards/IT-Frameworks ein vergleichbares IT-Compliance-Niveau wie mit CobiT erreicht werden kann. Nachfolgende Tabelle (siehe Tab. D-1) veranschaulicht den Auszug aus einer Mapping-Tabelle der ISACA.

CobiT (Auszug für Prozess „DS5 Ensure Systems Security“)	**ITIL**
DS5.1 Management of IT security	• SD 4.6 Information security management • SO 5.13 Information security management and service operation
DS5.2 IT security plan	• SD 4.6.4 Policies/principles/basic concepts • SD 4.6.5.1 Security controls (high-level coverage, not in detail)

Tab. D-1: Auszug des Mappings zwischen CobiT und ITIL (ISACA 2008, S. 47-48)

Da aber die inhaltlichen Überschneidungen unterschiedliche Ausprägungen (z. B. vollständig, teilweise, minimal) einnehmen können, ist eine allgemein gültige Transformation in einen CobiT-Reifegrad nicht möglich bzw. sinnvoll. Die Transformationsregeln (in der auch eine Priorisierung vorzunehmen ist) müssen fallbasiert für jede dynamische Föderation festgelegt werden. Als Ergebnis lässt sich folgende allgemeine Policy-Struktur (siehe Tab. D-2) festhalten.

CobiT-Prozess [z]	ITIL	ISO/IEC 27002	IT-Grundschutz	…
Reifegrad 1_z	a_1 von y_{ITIL}	b_1 von y_{ISO}	c_1 von $y_{IT\text{-}GS}$	…
Reifegrad 2_z	a_2 von y_{ITIL}	b_2 von y_{ISO}	c_2 von $y_{IT\text{-}GS}$	…
Reifegrad 3_z	a_3 von y_{ITIL}	b_3 von y_{ISO}	c_3 von $y_{IT\text{-}GS}$	…
Reifegrad 4_z	a_4 von y_{ITIL}	b_4 von y_{ISO}	c_4 von $y_{IT\text{-}GS}$	…
Reifegrad 5_z	a_5 von y_{ITIL}	b_5 von y_{ISO}	c_5 von $y_{IT\text{-}GS}$	…

Tab. D-2: Allgemeine Policy-Struktur

- z: beliebiger CobiT-Prozess
- y: Gesamtmenge aller abgeleiteten Anforderungen je Standard/IT-Framework auf Basis von Mapping-Tabellen
- a, b, c: Teilmenge der zu erfüllenden Anforderungen je Reifegradlevel, wobei a, b, c $\leq$ y

Um beispielsweise CobiT-Reifegrad 2 zu erreichen, ist äquivalent bei der Verwendung von ITIL die Teilmenge a_2 aus der Gesamtmenge der Anforderungen y_{ITIL} umzusetzen.

15.6 Anwendung der Ergebnisse auf das Szenario e-Car Net

Nach der Analyse der vier vorgestellten Standards/IT-Frameworks und der Schlussfolgerung, dass CobiT die aufgestellten Anforderungen am besten erfüllt, wird in diesem Abschnitt die beispielhafte Anwendung von CobiT im Kontext des Szenarios e-Car Net (Kapitel 2, sowie Leunig et al. 2010) veranschaulicht. In diesem Zusammenhang erfolgt zudem die Anwendung einer Policy.

Konkret liegt der Fokus auf dem Aspekt der Auslieferung der e-Cars aus dem Teilszenario B, dem Absatz von PKWs mit Elektroantrieb (e-Cars) (Leunig et al. 2010, S. 13). Dabei wird angenommen, dass die Auslieferung des e-Cars nicht von einem einzigen Logistikdienstleister durchgeführt wird, sondern von mehreren in Form einer sich ad-hoc bildenden Föderation. Dieses Szenario wird in nachfolgender Abbildung (siehe Abb. D-6) veranschaulicht, welche auch Gegenstand des 7. Kapitels „Effizienzsteigerung hochflexibler Geschäftsprozesse mittels Simulation“ ist.

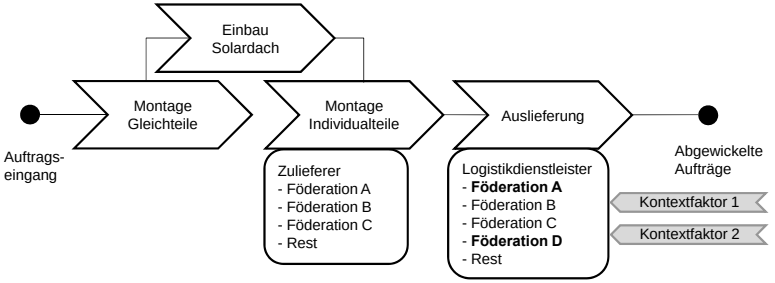

Abb. D-6: Darstellung des Wertschöpfungsnetzes der e-Car AG (siehe Kapitel 7)

In diesem beispielhaften Fall fordert die e-Car AG bei der Ausschreibung des Transportauftrages, dass diejenigen Logistikdienstleister, welche das e-Car zum Kunden befördern wollen, entweder einen Reifegrad von mindestens 3 (die Skala reicht von 0 „nicht existent“ bis 5 „optimiert“) bei dem CobiT-Prozess „DS5 Gewährleiste Systemsicherheit“ (engl. Ensure Systems Security) nachweisen oder den Beleg für ein vergleichbares IT-Compliance-Niveau bei Verwendung eines anderen Standards/IT-Frameworks (Transformationsregeln wurden hierfür in der Policy festgelegt) erbringen müssen. Der Grund für diese Forderung liegt in der Übertragung von schützenswerten Kundeninformationen von einem Föderationsteilnehmer auf den nächsten.

Auf die Ausschreibung zum Transport des e-Cars haben sich sechs Logistikdienstleiter beworben. Das Ergebnis der Sichtung ihrer eingereichten Unterlagen zeigt auf, dass vier Bewerber CobiT, einer ITIL und einer IT-Grundschutz anwenden. Um das Beispiel nicht unnötig zu komplizieren, wird die generelle Annahme getroffen, dass die Entscheidung wer den Auftrag bekommt nur auf der Grundlage der Ausprägung des jeweiligen eingesetzten Standards/IT-Frameworks getroffen wird. In dem vorliegenden Fall fällt die Wahl auf den Transporteur, welcher einen Reifegrad von 4 bei dem CobiT-Prozess DS5 aufweist. Alle anderen Bewerber schneiden schlechter ab.

Der ausgewählte Logistikdienstleister transportiert das e-Car jedoch nicht direkt zum Kunden, sondern vergibt einen Teil der Strecke an einen anderen Spediteur, wobei auch hier die aufgestellte Anforderung der e-Car AG gilt. Auf diese Ausschreibung bewerben sich vier Transporteure. Aus deren übermittelten Unterlagen wird ersichtlich, dass zwei Logistikdienstleister die Anforderung grundsätzlich nicht erfüllen. Bei den verbliebenden Bewerbern weist ein Spediteur den geforderten Reifegrad von 3 bei dem CobiT-Prozess DS5 nach. Der letzte Trans-

porteur verwendet kein CobiT, hat aber ITIL im Einsatz. Auf Basis der Anwendung der definierten Transformationsregeln in der Policy kann dieser jedoch einen Reifegrad von 4 nachweisen, wodurch die Entscheidung für den Auftrag zu seinen Gunsten fällt.

Anhand dieses einfachen Beispiels wird deutlich, wie mit Verwendung einer Policy (auf Basis von CobiT in Zusammenhang mit Mapping-Tabellen) über das gesamte Wertschöpfungsnetz ein vergleichbares IT-Compliance-Niveau erreicht werden kann, ohne die Flexibilität hinsichtlich der Teilnahmemöglichkeit an dem Wertschöpfungsnetz zu stark einzuschränken.

Grundsätzlich ist in diesem Zusammenhang noch das Problem zu berücksichtigen, dass sich eine Überprüfung des ausgewiesenen Reifegrads zum einen aufgrund der hGP-Eigenschaften (Pütz et al. 2009, S. 1) und zum anderen aufgrund eines gewissen, vorherrschenden Zeitdrucks als äußerst schwierig gestaltet und sich somit die jeweiligen Partner gegenseitig vertrauen müssen.

Jedoch entsteht das Vertrauen in der Regel erst im Laufe einer länger andauernden Geschäftsbeziehung. Im Kontext von hGP schränkt dieses Vorgehen die Hochflexibilität in erheblichem Maße ein, da der nächste Kopplungspartner gerade aufgrund der unvollständigen Planbarkeit sowie der Überlappung von Planung und Ausführung ein Unternehmen sein kann, mit dem noch niemals zuvor eine Geschäftsbeziehung bestanden hat. Somit ist das Entgegenbringen eines „blinden“ Vertrauens ohne jegliche Grundlage geradezu vermessen und faktisch grob fahrlässig.

Zur Lösung dieser Problemstellung sind folgende zwei Ansätze denkbar:

- Als vertrauensbildende Maßnahme bestätigt die **Interne Revision** eines Unternehmens den ermittelten Reifegrad. Aufgrund ihrer unabhängigen Stellung in der Organisation und ihres Aufgabenspektrums (spezifiziert unter anderem in § 91 Abs. 2 AktG, § 25a Abs. 1 KWG und den Mindestanforderungen an das Risikomanagement), insbesondere der Kontrolle der ordnungsgemäßen Abläufe von Prozessen und der Einhaltung geltender Gesetze und Regularien, liefert die Interne Revision durch die Beglaubigung der zu übermittelnden Angaben damit einen vertrauensfördernden Beitrag, welcher entscheidend für die Kopplung sein kann.
- Falls ein Unternehmen keine Interne Revision besitzt, muss die Bestätigung des jeweiligen Reifegrads durch eine vertrauenswürdige **dritte Instanz** (Trusted Third Party) erfolgen.

15.7 Zusammenfassung

Die nachweisliche Einhaltung von IT-Compliance-Vorschriften insbesondere im Kontext von hGP stellt die Unternehmen vor komplexe Herausforderungen. Dies wurde auch durch die Darstellung und Erläuterung einiger ausgewählter IT-spezifischer Gesetze und Regularien veranschaulicht. Die Anwendung von Standards/IT-Frameworks kann bei der Bewältigung der Herausforderungen sehr hilfreich sein, allerdings nur wenn dabei eine Berücksichtigung der hGP-Eigenschaften stattfindet. Um diesem Aspekt Rechnung zu tragen, wurden entsprechende Anforderungen aufgestellt, anhand derer eine Analyse von vier ausgesuchten Standards/IT-Frameworks erfolgte.

Die durchgeführte Untersuchung hat ergeben, dass CobiT unter den vorgestellten Alternativen am besten die definierten Kriterien erfüllt und damit für den hGP-Kontext ein geeignetes Mittel darstellt. Insbesondere durch das integrierte Reifegradmodell wird zum einen eine hohe Transparenz erzielt und zum anderen eine flexible inhaltliche Ausgestaltung ermöglicht. Nur hinsichtlich der Elastizität und der Werkzeug-Unterstützung sind bei CobiT noch Schwächen vorhanden. Zudem wurde jedoch die Erkenntnis gewonnen, dass die alleinige Fokussierung auf CobiT die Flexibilität zu stark einschränken würde, da auch für potenzielle Teilnehmer, die nicht CobiT verwenden, die Möglichkeit bestehen muss, an dem Wertschöpfungsnetz zu partizipieren. Dies kann mit Hilfe einer Policy erreicht werden, welche auf Basis von Mapping-Tabellen geeignete individuelle Transformationsregeln beinhaltet und somit für eine gewisse Vergleichbarkeit zwischen den Standards/IT-Frameworks sorgt. Weiterhin hat die exemplarische Anwendung einer Policy auf das Szenario e-Car Net verdeutlicht, wie der Ablauf bei einem sich ad-hoc bildenden organisationsübergreifenden Wertschöpfungsnetz ausgestaltet sein könnte.

15.8 Literatur

Bertele M, Lehner F (2008) IT-Compliance: Rechtliche Aspekte des IT-Managements. Darstellung rechtlicher Aspekte – organisatorische, technische und personelle Maßnahmen – Rahmenkonzepte zur Umsetzung, 1. Aufl. VDM Verlag Dr. Müller, Saarbrücken

Bitterli PR (2006) Das CobiT-Framework für IT-Governance. In: Bitterli PR (Hrsg) Praxishandbuch CobiT – IT-Prozesse steuern, bewerten und verbessern, 1. Aufl. Symposion Publishing, Düsseldorf

Bretz J, Hinssen J, Kolb A, Martin G, Peltier G, Rosenberger P (2007) IT-Sicherheitsmanagement in Banken und Sparkassen: Implementierung, technisch-organisatorische Umsetzung und Überwachung im Lichte gestiegener, gesetzlicher und bankenaufsichtlicher Anforderungen, 1. Aufl. Finanz Colloquium Heidelberg, Heidelberg

Bundesamt für Sicherheit in der Informationstechnik (2009) IT-Grundschutz-Kataloge – 11. Ergänzungslieferung, Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile. Abruf am 2011-02-04

Bundesdatenschutzgesetz (2009) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814)

Deutscher Bundestag (1998) Bundestagsdrucksache 13/9712. http://dip21.bundestag.de/dip21/btd/13/097/1309712.pdf. Abruf am 2011-02-04

DIN Deutsches Institut für Normung e. V. (2007) DIN EN 45020:2007-03 (D) – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004), 8. Aufl. Beuth Verlag, Berlin

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (1998) in der Fassung der Bekanntmachung vom 27. April 1998 (BGBl. I S. 786-794)

Gaulke M (2010) Praxiswissen COBIT – Val IT – Risk IT. Grundlagen und praktische Anwendung für die IT-Governance, 1. Aufl. dpunkt.verlag, Heidelberg

Gola P, Schomerus R (2010) BDSG – Bundesdatenschutzgesetz: Kommentar, 10. Aufl. Verlag C. H. Beck, München

Hauschka CE (2007a) Einführung. In: Hauschka CE (Hrsg) Corporate Compliance – Handbuch der Haftungsvermeidung im Unternehmen, 1. Aufl. Verlag C. H. Beck, München, 1-25

Hornby AS (2007) Oxford Advanced Learner's Dictionary, 7. Aufl. Oxford University Press, Oxford

International Organization for Standardization (2005) ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security management, 1. Aufl., Genf

ISACA (2008) Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf. Abruf am 2011-03-24

IT Governance Institute (2007) CobiT 4.1. http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf. Abruf am 2011-01-27

Johannsen W, Goeken M (2007) Referenzmodelle für IT-Governance – Strategische Effektivität und Effizienz mit COBIT, ITIL & Co, 1. Aufl. dpunkt.verlag, Heidelberg

Klotz M, Dorn DW (2008) IT-Compliance – Begriff, Umfang und relevante Regelwerke. In: HMD – Praxis der Wirtschaftsinformatik (2008) 263:5-14

Klotz M (2009) IT-Compliance – Ein Überblick, 1. Aufl. dpunkt.verlag, Heidelberg

Leunig B, Wagner D, Ferstl OK (2010) Hochflexible Geschäftsprozesse in der Logistik – ein Integrationsszenario für den Forschungsverbund forFLEX. Bayerischer Forschungsverbund Dienstorientierte IT-Systeme für hochflexible Geschäftsprozesse (forFLEX), Bericht-Nr. forFLEX-2010-001.

Office of Government Commerce (2007a) ITIL – What is it? / How does it work? http://www.ogc.gov.uk/guidance_itil_4671.asp. Abruf am 2011-02-21

Office of Government Commerce (2007b) ITIL – Books and resources. http://www.ogc.gov.uk/guidance_itil_4899.asp. Abruf am 2011-02-21

Ohrtmann N (2009) Compliance – Anforderungen an rechtskonformes Verhalten öffentlicher Unternehmen, 1 Aufl. LinkLuchterhand, Köln

Ponemon Institute (2011) The True Cost of Compliance – A Benchmark Study of Multinational Organizations. http://www.tripwire.com/ponemon-cost-of-compliance/pressKit/True_Cost_of_Compliance_Report.pdf. Abruf am 2011-02-08

Pütz C, Wagner D, Ferstl OK, Sinz EJ (2009) Geschäftsprozesse in Medizinischen Versorgungszentren und ihre Flexibilitätsanforderungen – ein fallstudienbasiertes Szenario. Bayerischer Forschungsverbund Dienstorientierte IT-Systeme für hochflexible Geschäftsprozesse (forFLEX), Bericht-Nr. forFLEX-2009-001.

Rudd C (2006) ITIL – the IT Infrastructure Library. In: van Bon J, Verheijen T (Hrsg.) Frameworks for IT Management, 1. Aufl. Van Haren Publishing, Zaltbommel

Schubert S (2008) Wettbewerbsvorteile durch Vereinheitlichung am Beispiel der europäischen Schienenfahrzeugindustrie, Dissertation, Juristischen und Wirtschaftswissenschaftlichen Fakultät der Martin-Luther-Universität Halle-Wittenberg. http://sundoc.bibliothek.uni-halle.de/diss-online/08/08H095/prom.pdf. Abruf am 2011-02-14

Schuppener J, Tillmann W (1999) KonTraG: Auswirkungen auf Kreditgeschäft und Bonitätsprüfung. In: Kreditpraxis (1999) 2:20-23

Sewera S (2005) Referenzmodelle im Rahmen von IT-Governance – CobiT ITIL MOF, Seminararbeit, Wirtschaftsuniversität Wien. http://www.ai.wu.ac.at/~koch/courses/wuw/archive/inf-sem-ss-05/referenzmodelle.pdf. Abruf am 2011-01-26

Shuja AK (2011) ITIL: Service Management Implementation and Operation, 1. Aufl. Auerbach Publications, Boca Raton

Speichert H (2007) Praxis des IT-Rechts – Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung. In: Fedtke S (Hrsg) Praxis des IT-Rechts – Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, 2. Aufl. Vieweg Verlag, Wiesbaden

Trub G, Olski L (2008) Global report on the status of IT compliance processes. http://ca.com/files/IndustryResearch/gmg-globalcompliancereport.pdf. Oktober 2008, Version 2. Abruf am 2011-01-26

van Bon J, Verheijen T (2006) Frameworks for IT Management, 1. Aufl. Van Haren Publishing, Zaltbommel